INTRODUZIONE

L'attuale periodo storico, la cui promessa è: apportare innovazioni alla vita umana, più velocemente di qualsiasi età precedente; ha contribuito ad un netto progresso nell'ambito sociale, culturale e lavorativo; la nascita dei moderni computer, alla portata di tutti, hanno drasticamente cambiato il modo di vivere della collettività, semplificando la vita di tutti i giorni. Oltre ogni dubbio, l'avanzamento tecnologico porta con sé l'inevitabile bisogno da parte del legislatore di creare un complesso di norme volte a fondare un sistema legislativo che assicuri la protezione di quei beni giuridici che rischiano inevitabilmente di essere compromessi tramite l'utilizzo "malevolo" di tali strumenti.

Inizialmente non era prevista alcuna tutela avverso i reati informatici, in quanto non erano considerati un pericolo per la società: a causa della scarsa conoscenza del fenomeno, tali delitti erano considerati frutto di azioni isolate e pertanto prive di rilevanza.

Nell'ultimo decennio, i mezzi informatici sono divenuti un fenomeno di massa, viene abbandonata la concezione della scarsa rilevanza di tali fatti e nasce pertanto un'attenzione peculiare verso quest'ultimi. In questo elaborato saranno analizzati, innanzitutto, proprio i progressi normativi degli ultimi anni, aventi lo scopo di reprimere le condotte criminose in materia di reati informatici.

Nel secondo capitolo saranno analizzate le fattispecie delittuose previste all'interno del codice penale, tenendo conto della normativa

vigente anche a livello sovranazionale; saranno trattati i reati elaborati in un'ottica anticipatoria della tutela penale, prendendo in considerazione le cd. norme di "sbarramento", nonché, una classificazione che tiene conto dei soggetti coinvolti e del bene giuridico leso, elementi imprescindibili al fine di delineare le numerose tipologie di reato che, ad oggi, sono previste nel novero dei comportamenti antigiuridici.

Nell'ultimo capitolo verrà effettuata un accurata analisi delle riforme introdotte con la legge 15 febbraio 2012, n.12, grazie alla quale sono state introdotte alcune nuove disposizioni in materia di confisca dei beni informatici e telematici utilizzati per la commissione di reati informatici e di destinazione dei medesimi beni, tenendo conto delle posizioni dottrinarie in tal senso.

CAPITOLO PRIMO
I REATI INFORMATICI: CLASSIFICAZIONE, EVOLUZIONE STORICA, BENI GIURIDICI

1.1 I REATI INFORMATICI: PROFILI GENERALI

Il reato informatico è un crimine tecnologico compiuto servendosi di supporti digitali, informatici o telematici, al fine di sottrarre, compromettere o distruggere beni e/o informazioni riservate.

Autorevole dottrina ha correttamente evidenziato tre aspetti principali: 1) la condotta ed i mezzi utilizzati; 2) l'oggetto materiale su cui ricade la condotta; 3) l'esistenza di particolari beni giuridici.

Per quanto attiene al primo aspetto, la condotta consiste nel danneggiare, manipolare, alterare tanto i beni che gli strumenti informatici e telematici[1].

Per quanto concerne il secondo aspetto, ossia l'oggetto materiale sul quale ricade la condotta, non si tratta soltanto di una *res* fisicamente tangibile, ma tale nozione va estesa a dati, informazioni o programmi. La peculiarità dei reati informatici ha portato la dottrina a configurare nuove figure di beni giuridici, considerati meritevoli di tutela, dotati di una loro completa autonomia rispetto a quelli preesistenti tra i quali quello dell'integrità di dati o programmi. É stato così elaborato il concetto di domicilio informatico.

É stata abbandonata la concezione originaria secondo la quale i reati informatici presupponevano particolari conoscenze tecnologiche a livello hardware e software; modello elaborato negli Stati Uniti, abbandonato a seguito di studi svolti a livello sovranazionale i quali affermano che: i Computer Crime sono figure di reato che concernono semplicemente l'informatica.

1.2 COMPUTER CRIME E CYBER CRIME: DIFFERENZE.

La diffusione della rete internet a metà degli anni Novanta, tecnologia utilizzata inizialmente soltanto a livello militare per scopi nettamente diversi da quelli utilizzati oggi dalla popolazione civile, ha contribuito, da un lato, ad una certa evoluzione sociale, culturale ed economica ma,

[1] MAURIZIO FUMO *La condotta nei reati informatici, Archivio Penale* settembre–dicembre 2013 fascicolo 3 anno LXV.

ha portato con sé anche notevoli aspetti negativi derivanti dall'uso criminoso di tali strumenti.

È emerso così un nuovo tipo di criminalità: il *cyber crime*, connesso al fenomeno di internet.

Occorre precisare che la macrocategoria dei reati informatici si suddivide in due sottoinsiemi: *cyber crime e computer crime.*

I *computer crime* contengono gli elementi tipici dei reati informatici (modalità di attuazione, oggetto su cui ricade la condotta, lesione dei particolari beni giuridici.)

Rientrano nel *Cyber crime* tutti quegli atti o fatti commessi tramite l'utilizzo della rete internet.

A titolo esemplificativo, rientrano nel *cyber crime*, gli atti di diffamazione commessi tramite l'utilizzo della rete internet, così come il reato di riciclaggio di denaro a mezzo di rete, cd. *cyberlaundering.*

Tra la cerchia dei reati informatici sono previste anche quelle figure criminose nelle quali non si porta a compimento il fatto reato, trattandosi di condotte di natura preparatoria accessoria o strumentale.[2]

1.3 L'EVOLUZIONE NORMATIVA DEI REATI INFORMATICI IN ITALIA: LE PRIME FIGURE DI REATO

La prima fattispecie riguarda "l'elaborazione dei dati", contemplata nell'art. 420 c.p. come novellato dall'art.1 dl. 21 marzo 1978 n.59, intervento in materia di terrorismo, a seguito dell'attentato al centro di

[2] L.PICOTTI*, La tutela penale della persona e nuove tecnologie dell'informazione*, Cedam, 2013 p.55

elaborazione dati della motorizzazione civile[3]. Il legislatore interviene al fine di incriminare in modo più grave il danneggiamento di impianti di pubblica utilità, di ricerca ed elaborazione dei dati, rispetto alla fattispecie di danneggiamento comune.

Tale norma diviene oggetto di revisione in seguito alla creazione di un vero e proprio complesso normativo all'interno del codice penale italiano, in materia di reati informatici, che avverrà nel 1993 con legge n. 547.

Prima, nel 1981, era disciplinato il delitto di comunicazioni o uso da parte di un pubblico ufficiale di dati ed informazioni in violazione della disciplina o dei fini previsti nella nuova normativa in tema di Pubblica Sicurezza[4].

Nel 1991, nell'ambito della legislazione speciale, si interviene per ostacolare l'uso del denaro contante con lo scopo di combattere il riciclaggio, viene inserita una figura di reato che punisce chi utilizza indebitamente carte di credito o di pagamento o altre analoghe carte che abilitino al prelievo di denaro contante o alla prestazione di beni o servizi ovvero la loro falsificazione od alterazione o il possesso, la cessione, l'acquisto di carte di tale tipo o documenti, se di provenienza illecita, o comunque falsificati o alterati.

A seguito del d.lgs. 29 dicembre 1992 n. 518, attuativo della direttiva CEE n. 91/250 del 14 maggio 1991 con riguardo alla tutela giuridica dei programmi per l'elaboratore, si ha un punto di svolta, che

[3] Si trattava, in particolare, di un attentato volto ad evitare il riconoscimento della falsità delle targhe apposte a veicoli rubati e poi utilizzati a scopi delittuosi.
[4] Art. 12 l. n.121/1981

rappresenta un intervento di natura sistematica, pur sempre nell'ambito della legislazione speciale.

Un anno dopo, a seguito delle raccomandazioni del Consiglio d'Europa, il legislatore nazionale interviene con la già citata legge n. 547, la quale apporta "modificazioni ed integrazioni alle norme del codice penale e di procedura penale in materia di criminalità informatica", una legge indispensabile al fine di contrastare gli atti criminosi commessi via computer o web, ovvero le fattispecie di danno ai sistemi informatici altrui, che la legislazione tradizionale non poteva descrivere efficacemente, se non tramite un'interpretazione in chiave evolutiva, andando però ad inficiare i principi di legalità, tassatività e determinatezza, capisaldi del diritto penale.

Gli strumenti giuridici di cui disponeva il giudice, non erano idonei a sanzionare i nuovi comportamenti *contra-legem* che iniziavano a verificarsi sul piano internazionale, nacquero così notevoli pressioni volte a ottenere una disciplina che assicurasse una risposta positiva concreta.

1.4 LA CONVENZIONE DI BUDAPEST SUL CYBERCRIME E LA SUA ATTUAZIONE

In un contesto in cui le società fanno sempre più affidamento sulle informazioni e sulla tecnologia, diventano sempre più vulnerabili al rischio della criminalità informatica.

La Convenzione sulla criminalità informatica di Budapest offre una risposta a tale rischio, non solo in Europa ma anche a livello globale:

attraverso il suo Programma sulla criminalità informatica, il Consiglio d'Europa fornisce assistenza tecnica ai paesi di tutto il mondo.[5]

Tale Convenzione, ha lo scopo di fornire un grado significativo di tutela, avverso i beni giuridici lesi dai fenomeni di *cyber-crime.*

La Convenzione prevede una serie di principi per agevolare gli Stati aderenti a conformarsi agli standard di tutela.

Viene previsto un importantissimo strumento, ovvero, un meccanismo di cooperazione tra gli organismi nazionali e internazionali.

L'accordo ha lo scopo di fornire la definizione giuridica di diverse terminologie, ad esempio la nozione di sistema informatico (da intendersi come qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico dei dati sulla base delle indicazioni fornite dal programma di software); la nozione di dati informatici (qualsiasi tipo di rappresentazione di fatti, informazioni o concetti idonei ad essere oggetto di trattamento ed elaborazione da parte di un programma o di un sistema informatico).

Il testo suggerisce agli Stati membri, un adattamento a livello normativo, di norme volte a sanzionare le condotte tipiche di aggressione ai sistemi informatici.

Gli Stati vengono invitati a punire tali fattispecie con "pene effettive, proporzionate e dissuasive, con la possibilità, di prevedere misure limitative la libertà personale[6].

[5] *Council of Europe action against Cybercrime, www.coe.int*
[6] Art. 13 della Convenzione

Nel testo della Convenzione, è prevista la responsabilità a carico delle persone giuridiche, nel caso in cui le persone fisiche abbiano commesso i delitti informatici con l'intento di soddisfare un interesse o raggiungere un vantaggio dell'ente collettivo, al quale sono legati da un rapporto di appartenenza o dipendenza.

Inoltre, le disposizioni procedurali in tema di indagini e giurisdizione, contenute nell'articolo 22 della Convenzione, si occupano di stabilire le modalità di attribuzione della competenza e della giurisdizione ad uno Stato, in caso di delitto informatico.

Sul piano nazionale, il cammino che porterà alla legge di ratifica n. 58/2008 non risulta tortuoso o complesso.

Il disegno di legge, presentato nel 2007, viene trasmesso alla Camera il 19 febbraio 2008, con il consenso "sostanzialmente" unanime, con un solo emendamento; il 20 febbraio viene approvato e trasmesso al senato; il voto finale è del 27 febbraio 2008.

Il procedimento di approvazione è effettivamente rapido, ma, porta con sé notevoli lacune ed incongruenze nella novella del legislatore, che ha voluto adeguare l'ordinamento italiano alle disposizioni del consiglio d'Europa nel più breve tempo possibile.

In sintesi, le modifiche apportate dalla 58/2008 possono essere ricomprese in una serie di sotto-gruppi: modifiche in materia di falsità informatiche (dall'intervento definitorio di documento informatico alla nuova fattispecie di false dichiarazioni al certificatore e alla nuova configurazione del delitto di frode informatica), novelle concernenti i delitti contro la sicurezza e l'integrità di dati e sistemi (la riformulazione dell'art 615 quinquies, le modifiche al reato di danneggiamento di dati

informatici, la nuova figura del danneggiamento di sistemi informatici e telematici, l'abrogazione del delitto di attentato informatico e l'inserimento delle fattispecie di danneggiamento di dati di pubblica utilità e danneggiamento di sistemi di pubblica utilità), la responsabilità da reato degli enti per i reati informatici.

1.5 REATI INFORMATICI E BENI GIURIDICI: VISIONE UNITARIA O PLURALISTICA?

Ancora oggi, il nostro ordinamento risulta privo di un sistema organico che disciplini il microcosmo dei reati informatici.
Non sono mancati in dottrina tentativi volti ad individuare un unico bene giuridico tutelato attuando una sorta di *reductio ad unum*.
Secondo alcuni autori sarebbe percepibile una dimensione unitaria del fenomeno come prodotto della tecnologia informatica telematica cibernetica; ciò al fine di individuare un unico oggetto di tutela che consista nell'affidabilità e sicurezza del ricorso alla tecnologia informatica telematica e cibernetica.
Il legislatore disciplina la materia sia nel codice penale che nella legislazione speciale.
Risulta evidente che i reati informatici siano stati collocati all'interno di titoli e capi preesistenti ovvero già preposti alla tutela di determinati beni giuridici.
Occorre individuare quali possano essere i beni giuridici della persona meritevoli di tutela nell'ambito dei reati informatici. Picotti effettua una suddivisione in quattro macrocategorie sulla base dei beni protetti. Il

primo fa riferimento ad una dimensione esclusiva e sicura di riservatezza informatica. Viene affermato come, tentando un approccio diverso da quello meramente analogico che tende ad assimilare sul piano concettuale questi "nuovi beni giuridico-informatici" con quelli tradizionalmente intesi, debba essere riconosciuto un carattere autonomo ed innovativo del predetto bene in questione. «La riservatezza informatica può essere compromessa da comportamenti potenzialmente dannosi nei confronti del sistema e dei dati, ovvero superando le misure di sicurezza ad esso relative, oppure, tramite l'accesso abusivo effettuato da soggetti privi di legittimazione, senza che sia richiesta la conoscenza di particolari e specifiche conoscenze di carattere informatico. La qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso ed alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza (chiavi fisiche o elettroniche, password, ecc.) apprestate dal titolare dello "i*us excludendi*", al fine di selezionare gli ammessi al sistema ed impedire accessi indiscriminati Il reato è integrato dall'accesso non autorizzato nel sistema informatico, ciò che di per sé mette a rischio la riservatezza del domicilio informatico, indipendentemente dallo scopo che si propone l'autore dell'accesso abusivo[7]» il mezzo di tutela consiste nel garantire la riservatezza e l'esclusività dell'accesso. Oltre all'accesso abusivo, vi sono ulteriori norme volte a tutelare il bene giuridico appena menzionato: l'articolo 615 *quater* punisce la

[7] Cass. pen. 2009, 7-8, 2828, *ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO - Configurabilità del reato - Irrilevanza dello scopo dell'accesso.*

detenzione la diffusione abusiva di codici di accesso, L'articolo 635 *bis* punisce la diffusione di dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico.

Per Quanto attiene al bene giuridico della riservatezza informatica, risulta di particolare importanza la decisione quadro dell'unione europea 205/222/GAI in il riferimento agli attacchi ai sistemi di informatici[8], allo scopo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione la legge, tenta il riavvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi informatici. La protezione di tale bene giuridico inoltre può trovare fondamento nell'articolo 7 della carta di Nizza, la quale prevede il rispetto della vita privata.

Un ulteriore bene giuridico meritevole di tutela è la riservatezza e sicurezza delle comunicazioni informatiche.

[8] Articolo 2: Accesso illecito a sistemi di informazione 1. Ciascuno Stato membro adotta le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato, almeno per i casi gravi. 2. Ciascuno Stato membro può decidere che i comportamenti di cui al paragrafo 1 siano punibili solo quando il reato è commesso violando una misura di sicurezza.
Articolo 3: Interferenza illecita per quanto riguarda i sistemi. Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili sia punito come reato se commesso senza diritto, almeno per i casi gravi.
Articolo 4: Interferenza illecita per quanto riguarda i dati. Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione sia punito come reato se commesso senza diritto, almeno per i casi gravi.